Preprint
UCRL-JC-137484

Progress in Gamma Ray Measurement Information Barriers for Nuclear Material Transparency Monitoring

J. K. Wolford, Jr. and G. K. White

This article was submitted to
Institute of Nuclear Materials Management 41st Annual Meeting, New Orleans, LA, July 16-20, 2000

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

July 3, 2000

PROGRESS IN GAMMA RAY MEASUREMENT INFORMATION BARRIERS FOR NUCLEAR MATERIAL TRANSPARENCY MONITORING

James K. Wolford[†], Jr., Mail Stop L-183, (925) 422-7236
Gregory K. White[‡], Mail Stop L-389, (925) 423-6732
Lawrence Livermore National Laboratory
P.O. Box 808, Livermore California, 94551, USA

ABSTRACT

Negotiations between technical representatives of the US and the Russian Federation in support of several pending nuclear arms and nuclear material control agreements must take account of the need for assurances against the release of sensitive information. Most of these agreements involve storing nuclear material and in some cases nuclear components from stockpile weapons in specially designed containers. Strategies for monitoring the agreements typically include measuring neutron and gamma radiation from the controlled items to verify declared attributes of plutonium or highly enriched uranium. If accurate enough to be useful, these measurements will contain information about the design of the component being monitored, information considered sensitive by one or both parties to the agreement. Safeguards have evolved to prevent disclosure of this information during inspections. These measures combine hardware, software, and procedural measures to contain the sensitive data, presenting only the results needed for verification. Custom features preserve data security and guard against disclosure in case of failure. This paper summarizes the general problem and discusses currently developing solutions for a high resolution gamma ray detection system. It argues for the simplest possible implementation of several key system components.

INTRODUCTION

In transparency monitoring, representatives of the monitoring country witness, or in some cases perform circumscribed measurements on controlled items. To mitigate the intrusiveness of these measurements and reduce concern over the unwanted disclosure of information, so-called information barriers have evolved. Briefly stated, an information barrier is a combination of hardware, computer software, and human procedures that:

1. Prevents the unintended release of sensitive information during an inspection.
2. Displays a simple but reliable and useful result to the inspector.
3. Allows checks on the integrity of the internal operations not visible during an inspection.

The need for information barriers is not unique to the inspections described in this paper. Indeed the concern over revealing too much information exists wherever intrusive inspection techniques are used on items or in facilities considered sensitive. Applying an information barrier to an inspection process forces designers to confront a dilemma; in hiding all but the essential indications from an inspector, one also hides data that would give some assurance that the internal operations proceeded as intended and that the measurement is therefore valid. As the sections below will demonstrate, thoughtful designs can help recover some of this lost assurance through features that simulate the actions and decisions of a human operator.

[†] e-mail: wolford1@llnl.gov
[‡] e-mail: white6@llnl.gov

CURRENT AND PLANNED MATERIALS AGREEMENTS

With the ratification of START II, the Russian Federal parliament (Duma) removed the diplomatic barriers to official discussion on the technical details of START III verification. Simultaneously progress is being made, albeit with less publicity, on agreements to store and safeguard excess nuclear material and material removed from dismantled weapons. Among them are the Trilateral Initiative, the Plutonium Production Reactor Agreement, and agreements for transparency at the Mayak fissile material storage facility. The Trilateral Initiative is the technical basis for an agreement to place excess fissile material in the US and the Russian Federation under IAEA safeguards. It includes provisions for symmetric inspections in both countries by the IAEA under the auspices of the nuclear Nonproliferation Treaty (NPT). The IAEA accepted the task of verifying and providing international confidence that these materials have been irreversibly removed from nuclear weapons programs. The initiative undertaken by DOE and Minatom was to develop monitoring approaches and technologies it could apply to US and Russian storage facilities. Work at Los Alamos National Laboratory (LANL) and Lawrence Livermore National Laboratory (LLNL) on preparing a prototype inspection system for Trilateral Initiative provided the original motivation for most of the ideas presented below.

Under another agreement, the US has supplied goods and services to build a new fissile material storage facility in Russia near the fuel processing site at Mayak. In return, the Russian Federation has agreed to enter stored material into a transparency regime monitored by the US. The US effort to develop measurement instrumentation with information barriers is known generically as Fissile Material Transparency Technology (FMTT) program. The FMTT demonstration instrument is the latest completed measurement system to incorporate an information barrier.

To address the issue of continued plutonium production in Soviet-era reactors, which are also necessary for power generation, the US and the Russian Federation have negotiated the Plutonium Production Reactor Agreement (PPRA). Methods for inspections under the PPRA are now under discussion.

THE EVOLUTION OF INFORMATION BARRIERS

The notion of an information barrier has existed for decades, though the nomenclature is more recent. Information barriers in some form have been used wherever adversaries have negotiated agreements that include inspections in the vicinity of sensitive information. Terms in the agreements dictate special features in the design of the measurement equipment to ensure that those inspections don't disclose more information than is necessary. Wolford and MacArthur give a perspective on information barriers in several previous applications.[1] Recent examples among US agreements include the Threshold Test Ban Treaty (TTBT) the Chemical Weapons Convention (CWC), and the attempt at an agreement for Mutual Reciprocal Inspections of nuclear weapons (MRI.) During TTBT negotiations, this measure was referred to as an *anti-intrusiveness device* (AID) and, despite its simplicity, was crucial to making a demonstration known as the joint verification experiment (JVE) a success.

Early successes and failures prompted continued development of measurement techniques that contained or lent themselves to the addition of an information barrier. Solutions to various facets of the problem have evolved at the US Department of Energy (DOE) national labs. Examples include:

- the Radiation Inspection System (RIS) developed by Sandia National Laboratories which uses the gamma ray spectrum from a sodium iodide detector to distinguish weapons-grade from reactor-grade plutonium.[2] The low resolution of the sodium iodide spectrum obscures many of the sensitive details.
- the Nuclear Material Identification System (NMIS) from Oak Ridge National Laboratory, suited for measurements on highly enriched uranium (HEU).[3] NMIS uses active interrogation, allowing the neutrons from a ^{252}Cf source to induce fission neutrons in the sample, and monitoring the emissions in a coincidence measurement.[‡]
- Brookhaven National Laboratory's CIVET (Controlled Intrusiveness Verification Technology) system, wherein engineers concentrated on the control and acquisition hardware with the goal of making it simple to authenticate.[4†]

These approaches have in common specificity of design; they address information protection of a specific measurement instrument, or they stress a particular requirement of information barriers in the abstract. The attribute system developed jointly by LANL and LLNL for the Trilateral Initiative offered the first modular solution that didn't rely on a full integration of the measurement instrument and the information barrier. MacArthur and Whiteson have documented requirements which have been provisionally agreed to by the three sides.[5] Preliminary design collaborations led to the creation of a prototype that is currently under review by the US government, the Russian Federation and the IAEA. The Example section describes the system developed for the pending FMTT demonstration, highlighting improvements that facilitate authentication.

DESIGN ELEMENTS

While an actual information barrier must be adapted to the measurement instrument it accompanies, some considerations require no knowledge of the type of measurement being performed. The US joint DOE-DOD Information Barrier Working Group identified 10 design bases for which to provide guidance.[6] Grouping them into functional categories, one may identify three high-level elements:

(1) A barrier to conceal the sensitive information gathered in a measurement, and from which the physical attributes of an inspected item are derived. This consists of some combination of hardware, software, and human procedures, and must work in both directions, shielding unintended signals originating both outside and inside the measurement system.

(2) A simplified display that indicates clearly the selected results of the measurement test as defined in the agreement, and nothing more. Accordingly, the display should be no more complex than is necessary to convey the result to the inspector.

(3) Enough autonomy to compensate for the lack of a human operator, both in monitoring the measurement and in safeguarding the data. The instrument must assure the reliability of its own measurements as well as protect the data resident during an inspection. In the event of failure or signs of tampering, this mechanism should erase all traces of sensitive data from the instrument and halt the inspection.

---

‡ Highly enriched uranium presents special challenges, since, unlike plutonium, it does not produce radiation with energies and intensities sufficient to penetrate optically thick absorbers. Thus passive radiation measurements on assembled weapons containing uranium are difficult.

† CIVET treats as paramount the desire to disclose exhaustively all hardware and software elements of a system, presumably making it easier for technical specialists to understand and trust its operation.

The first element encompasses any form of information transfer indicated in the setting. For example, if the unmodified instrument has a display that gives exhaustive information about the progress of a measurement (which many quality instruments do) then element 1 dictates that the display be disconnected, disabled, or covered up. If the inspector has close access to the instrument, one may additionally need to prevent it from transmitting or receiving signals of a mechanical (seismic, acoustic) or electromagnetic (RF, IR, or undeclared radioactive) origin. Commercial and government standards address each of these issues and can serve as a basis for discussion. Some of these measures are straightforward to incorporate into the design of the instrument, while others must be trusted to written authentication and inspection procedures as well as hardware and/or software.[†]

The second design element replaces the typical laboratory instrument interface with a simple set of indicators. If the derived attribute is not sensitive, then the value itself may be displayed, and a numerical readout is appropriate. Otherwise, the instrument's processor compares it to a negotiated threshold and displays instead a pass or fail for the comparison test. The threshold should be set at a value well outside the range likely to be encountered during measurements, so that normal statistical variations do not generate a pattern of passes and fails that effectively disclose the physical value. The exact implementation of the inspector's display should lend itself to authentication tests meant to verify that no incidental information is inadvertently or purposefully displayed. Examples include a bank of indicator lights or, for permanent records, a printed hardcopy containing the same simple results.

The third element ensures the integrity of the physical barrier by, for example, fitting any access doors with interlocks designed to withdraw power from the instrument and display whenever the enclosure is opened. Extending this idea, one could create a "security watchdog," which not only triggers a shutdown for a list of error conditions, but could also give a positive indication of status when it judges the system is functioning as intended. V. Poplavko of IPPE in Obninsk, Rs suggested just such a feature for the Trilateral Initiative measurement system. The function of the watchdog is to enforce a set of assertions that should obtain during normal operations, e.g., "the enclosure is sealed," "the enclosure is grounded," and "the processor received the neutron result in less than 10 minutes."

Figure 1 shows a block diagram illustrating the relationship among the 3 design elements. The acquisition system operates within a barrier, confining the sensitive data to a volume inaccessible to and obscured from the view of the inspector. The results appear on a display that reveals only the required attributes. The security watchdog monitors the status of factors affecting data protection and terminates the inspection, deleting all gathered data, if it detects a security threat.

In the next section, these design elements are exemplified in a hypothetical gamma ray spectroscopy instrument, which is similar in design to a portion of the FMTT prototype system. The specific design of the Trilateral system depends strongly, as does any system, on the circumstances of the agreement. These include the inspection attributes as well as arrangements for the custody of the hardware.

[†] One could conceive of a barrier composed entirely of written procedures, enforced by representatives from each country or organization participating in the agreement. Success in such an arrangement would depend on uncharacteristically flawless human action and would be labor intensive.

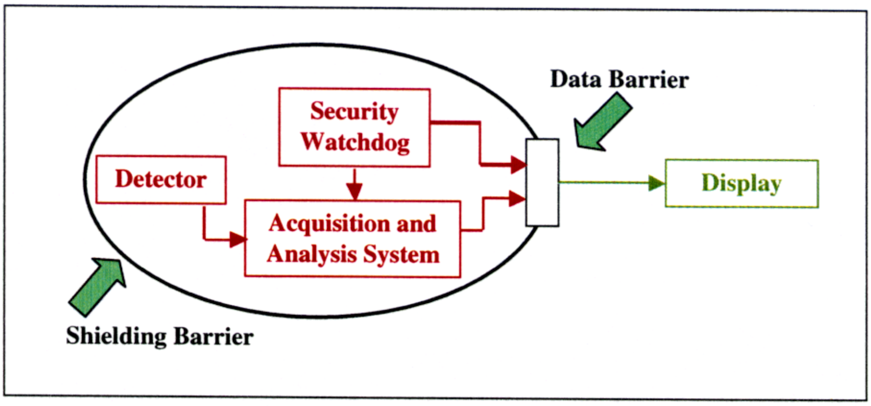

Figure 1. High level block diagram showing the interrelationship between the three design elements. Once the system derives its attribute results, they must pass through an isolation step before crossing the shielding barrier. The data barrier provides this isolation, interfacing to the display, and ensuring that the information contains only the agreed-to indications. The exact format of the display is shaped by the needs of the inspecting organizations. The security watchdog oversees the acquisition and analysis processes and shuts them down in case the barrier is breached.

EXAMPLE: INFORMATION BARRIER FOR GAMMA RAY MEASUREMENTS

Gamma ray spectroscopy is a common method of identifying the nuclides present in a sample. Knowledge of the continuum and proper spectral line intensities in a high-resolution measurement allows one to infer a wealth of information about the object being measured, including its constituents, their relative abundances, and a lower bound estimate of their masses, as well as information about the amount of intervening material (optical thickness.) Also, in a neutron-producing source such as plutonium, the presence of other significant elements can be inferred from evidence of their activation products. Clearly, much of this information lies outside the purview of transparency agreements. Fortunately some of the most useful attributes do not require information from the full spectrum for their derivation. Specifically lines for three of the attributes for the FMTT demonstration fall within narrow subintervals.

Since the role of the information barrier in gamma ray measurements is to pass only those attributes of the spectrum chosen for the inspection regime and to conceal all others, planners have an opportunity to protect most of the information *a priori*. Koenig at LLNL created software that used the plutonium lines between 630 and 670 keV to compute the ratio of ^{240}Pu to ^{239}Pu which distinguishes plutonium suitable for weapons from, for example, that intended for a reactor.[7] This tool, named "Pu600" for the range of spectral lines it uses, was adapted and enhanced by Luke for the requirements of the Trilateral Initiative and the FMTT program.[8,9] Archer and Luke developed similar methods, dubbed "Pu300" and "Pu900," for determining the time since separation and amount of oxide present in a sample respectively.[10] Figure 2 illustrates how relatively little information from the total spectrum is required for these calculations.

The requirement for "hands off" operation shifts the burden for performing a valid measurement from a knowledgeable operator to the instrument itself. The gamma ray measurement for FMTT takes place for a fixed count time and at a prescribed distance from the controlled items. Maintaining data quality and accommodating the full range of source intensities (a function of the mass and composition) possible under certain agreements requires an additional measure to ensure validity. Luke at LLNL solved this problem elegantly by designing an adjustable diaphragm (iris) with leaves made of tungsten approximately 1 cm thick. A stepper motor adjusts the iris aperture governed by consideration of the maximum allowable dead time. This ensures good counting statistics, and since the enclosure shrouds both the iris and the detector, the inspector is prevented from estimating the included solid angle of the detector face. Concerns expressed by the IAEA about the survivability of the Trilateral iris in field applications led Luke and his colleagues at LLNL (Archer, Mauger, and Lochner) to institute improvements for the FMTT mechanism and its drive train, thereby making it more robust.

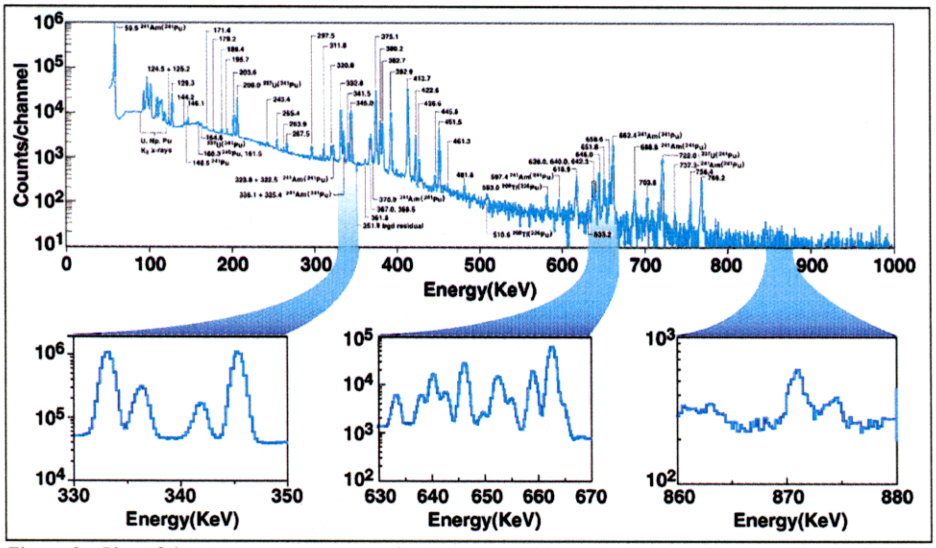

Figure 2. Plot of the gamma ray spectrum from a non-sensitive sample of plutonium containing several isotopes and decay products. The details illustrate the relatively narrow subintervals containing the spectral lines used in the attribute calculations known as Pu300, Pu600 and Pu900 respectively. (*Plot courtesy of Thomas B. Gosnell, LLNL.)*

For the security watchdog to protect the measurement data effectively, it must at the very least erase it by withdrawing power in case of anomalous events. In particular, the acquisition and analysis computer may contain no fixed magnetic media such as a hard or floppy disk. Consequently the boot process must read from some read-only media such as a PROM chip or CD-ROM. Also the processor memory must be volatile and decay quickly when powered down. And, since the measurement must occur without intervention, neither a keyboard nor a display may be connected. The computer's results are communicated via serial interface to an output module, which acts as the data barrier. White at LLNL has designed and built several such systems for the Trilateral Initiative and FMTT. They boot MS-DOS from CD-ROM (Trilateral) or PROM (FMTT) and create RAM disks from which to run the analysis software.

FUTURE CHALLENGES

Having established that information barriers can be trusted, in principle, to protect the sensitive information gathered in measurements of nuclear material, the US and Russian Federation must develop systems which not only work as intended but are façile enough in their design and operation to be accepted by the governments of both sides. This requires a reduction in overall complexity, down to the simplest instrument capable of performing its function reliably and autonomously. The authors see the greatest potential for improvement in the transition from adapted, generic laboratory instrumentation to more special purpose inspection equipment, and the greatest single challenge as an evolution away from stored programs and microprocessors toward pure hardware solutions.

SUMMARY

The technology of information barriers is primitive compared to the technology of radiation detection and data reduction. Nevertheless, relatively simple systems such as those described above and in the references have provided sufficient assurance to sustain negotiations. Indeed, the simplicity of the designs itself promotes confidence in their reliability. The specific implementation of an information barrier system will depend on the requirements of the inspection regime. Nevertheless, the three elements introduced here will always form its basis. More specific design influences include decisions about equipment origin and custody and the number and type of physical attributes to be collected. Ultimately, the success of such systems will depend on the active participation of the nations or organizations with a stake in the outcome.

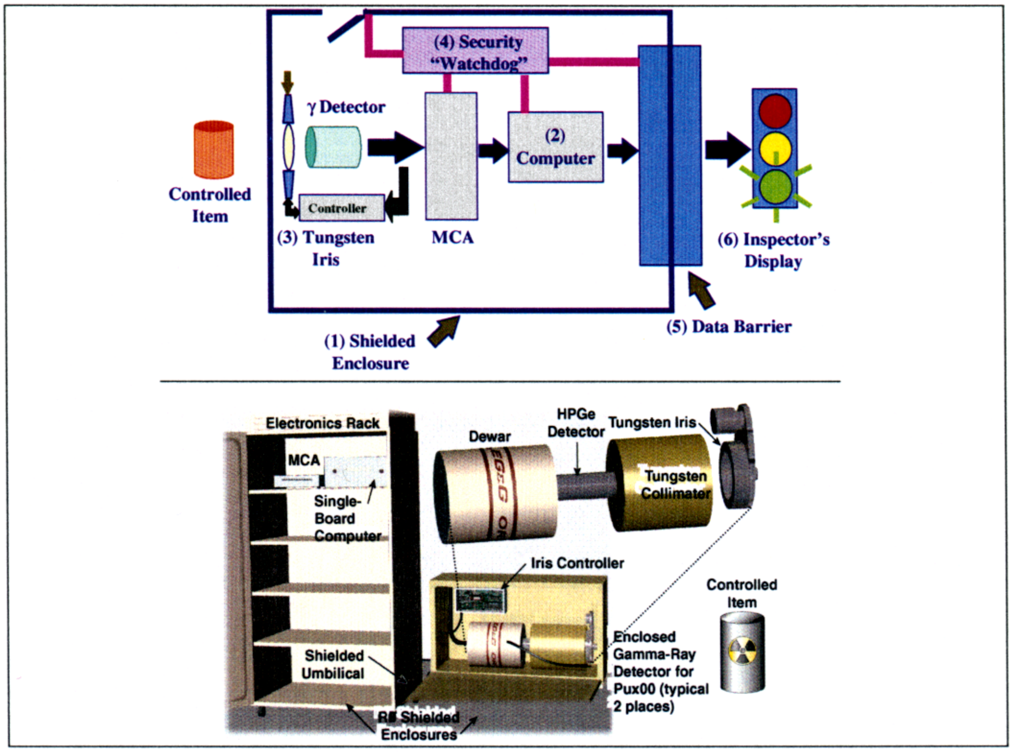

Figure 3. Block diagram and illustration of a hypothetical gamma ray inspection system with an information barrier. The key elements of the information barrier include: (1) opaque, grounded conducting enclosures, which prevent telltale EM emanations from the electronics; (2) simplified acquisition and analysis computer with most components on a single board; (3) tungsten iris, which opens and closes to optimize the live time of the measurement while keeping the included solid angle uncertain; (4) "Security watchdog," which activates on indications of events which threaten data security (e. g., opening of the enclosure); (5) data barrier, which isolates via optical fiber or some other one-way transmission path, and (6) the simplified user display.

ACKNOWLEDGMENTS

This work was completed by Lawrence Livermore National Laboratory for the U.S. Department of Energy under contracts W-7405-ENG-48.

REFERENCES

1. Wolford, J.K., and MacArthur, D.M., *Safeguards for Nuclear Material Transparency Monitoring*, Proceedings of SPIE Conference on Penetrating Radiation Systems and Applications, 19-23 July 1999, Denver Colorado, Vol 3769. LLNL internal document number UCRL-JC-134787.

2. Mitchell, D.J., Marlow, K.W., and Scott, H.L., *Application of a Low-Resolution Gamma-Ray Spectrometer for Nuclear Material Confirmation*, Proceedings of the Trilateral Technical Workshop, December 2-5, 1997, Livermore, California, p. 26.

3. Mattingly, J.K., Mihalczo, J.T., Valentine, T.E., Mullins, J.A., and Hughes, S.S., *Operational Use of NWIS for Storage of Weapon Components at the Oak Ridge Y-12 Plant*, ORNL Report No. Y/LB-15,943 R2, (1998).

4. Zuhoski, P., Foreman, L., and Vanier, P., *CIVET - Controlled Intrusiveness Verification Technology*, Brookhaven National Laboratory Internal Report.

5. MacArthur, D.W., and Whiteson, R.M., *Functional Requirements for a Prototype Inspection System and Information Barrier for the Trilateral Initiative*, Los Alamos National Laboratory, LA-UR-99-829 (1999).

6. The Joint DOE-DOD Information Barrier Working Group, *The Functional Requirements and Design Basis for Information Barriers*, Pacific Northwest National Laboratory, May 1999.

7. Koenig, Z.M., Carlson, J.B., Clark, D.L., and Gosnell, T.B., *Plutonium Gamma-Ray Measurements for Mutual Reciprocal Inspection of Dismantled Nuclear Weapons*, Proceedings of the 35^{th} Annual Meeting of the INMM, Vol. 22, 1152 (1995).

8. Luke, S.J., Carlson, J.B., Clark, D.L., Gosnell, T.B., and Koenig, Z.M., *Determining the Ratio of* ^{240}Pu *to* ^{239}Pu *by High-Resolution Gamma Ray Spectroscopy*, Proceedings of the Trilateral Technical Workshop, December 2-5, 1997, Livermore, California, p. 22.

9. Luke, S.J., Archer, D.E., and Gosnell, T.B., *Determination of Plutonium Isotopics for Arms Control and Nonproliferation*, Journal of Radioanalytical and Nuclear Chemistry (to appear), LLNL internal document number UCRL-JC-136625 (2000).

10. Archer, D. E., and Luke, S. J., *Pu300: A Measurement of Plutonium Age for Arms Control Transparency via Gamma Ray Spectroscopy*, Journal of Radioanalytical and Nuclear Chemistry (to appear), LLNL internal document number UCRL-JC-136626 (2000).